Last Time: Elementary properties of Divisibility.

Today: Generalize A little.

Reminder: $a \mid b$ when there is $m \in \mathbb{Z}$ w/ $b = am$.

Prop (Quotient-Remainder Theorem): Let $n, d \in \mathbb{N}_0$ ($\mathbb{Z}$) with $d \neq 0$. There exist unique $q, r \in \mathbb{N}_0$ ($\mathbb{Z}$) satisfying both $n = dq + r$ and $0 \leq r < |d|$.

Remarks: $n = dq + r$
- n: dividend
- q: quotient
- r: remainder

r is the remainder of n [under division by d]

q ~~//~~ quotient of n [under division by d]

instead of writing "under division by d", we sometimes say "modulo d", and call d the "modulus".

NB: There is a Quotient-Remainder Theorem for integers instead of just natural numbers...

NB: The version of QRT w/ the pink changes is left as an easy exercise...

NB: To prove QRT, we need a variant of induction called the Well-Ordering Principle.

Prop (Well-Ordering Principle): Every nonempty subset of $\mathbb{N}$ has a minimum element.

(i.e. if $\emptyset \neq S \subseteq \mathbb{N}$, then there is an $m \in S$ such that for all $s \in S$ we have $m \leq s$.)

The proof is by induction on the cardinality of S for finite S and by reduction to the finite case when S is infinite.

"Lemma"

Lem: If $S \subseteq \mathbb{N}$ is nonempty and finite, then S has a minimum.

pf(Lem): We proceed by induction on n, i.e. the cardinality of S.

Base Case: When $n = 1$, we have $S = \{s_1\}$ for some $s_1 \in \mathbb{N}_0$. Now $s_1 \leq s_1$, so $\min(S)$ exists and is s_1 in this case.

Inductive Step: [Suppose (for induction) we know that every subset of $\mathbb{N}$ having n elements has a minimum for some $n \geq 1$.] Suppose S has precisely $n+1$ elements. Thus

$$S = \{s_1, s_2, \cdots, s_n, s_{n+1}\}.$$

Consider $T = \{s_1, s_2, \cdots, s_n\}$, the first n listed elements of S. By the Inductive hypothesis,

T has a minimum element m. By Total Ordering of $\mathbb{N}$, [we know either $m \leq S_{n+1}$ or $S_{n+1} \leq m$].

* If $m \leq S_{n+1}$, then $m \leq S_i$ for all $1 \leq i \leq n$ (because $m = \min(T)$) and $m \leq S_{n+1}$, so $m \leq x$ for all $x \in S$ and $m = \min(S)$.

* If $S_{n+1} \leq m$, then for all $1 \leq i \leq n$, we have $S_{n+1} \leq m \leq S_i$ (by $m = \min(T)$), so $S_{n+1} = \min(S)$ (because we just showed $S_{n+1} \leq x$ for all $x \in S$). Hence, in all cases S has a minimum element, as desired.

Hence the inductive step holds.

Hence the lemma holds by mathematical induction ☑

pf (Well-Ordering Principle): Let $S \subseteq \mathbb{N}$ be arbitrary and nonempty. As S is nonempty, there is an element $e \in S$. Consider the set $T := \{t \in S : t \leq e\}$. Notice $e \leq e$ and $e \in S$ by assumption, so $e \in T \neq \emptyset$. Now $T \subseteq \{0, 1, 2, \cdots, e\}$, so T is finite (because it has at most $e+1$ elements). By the lemma, we may conclude T has a minimum element, $m \in T$.

On the other hand, $T \subseteq S$ yields $m \in S$. By construction of the set T, every element $x \in S$ satisfies either $x \in T$ or $x \notin e$ (i.e. $x > e$).

If $x \in T$, then $m \leq x$ because $m = \min(T)$.

If $x \notin T$, then $m \leq e < x$, so $m \leq x$. Hence, in either case $m \leq x$, so $m = \min(S) \in S$.

In particular, S has a minimum. ∎

Remark: The Well-Ordering Principle is Logically equivalent to weak mathematical induction. This formulation lends itself nicely to making proofs by contradiction...

Prop (Quotient-Remainder Theorem): Let $n, d \in \mathbb{N}_0$ with $d \neq 0$. There exist* unique* $q, r \in \mathbb{N}_0$ satisfying both $n = dq + r$ and $0 \leq r < d$.

↑ forces uniqueness...

pf: Let $n, d \in \mathbb{N}_0$ with $d \neq 0$. Thus $d > 0$.

Existence: (WTS: $\exists\ q, r \in \mathbb{N}_0$ w/ $n = dq + r$ and $0 \leq r < d$).

Consider the set $R = \{x \in \mathbb{N}_0 : \exists\ y \in \mathbb{N}_0 [n = dy + x]\}$.

Note $n \in R$ because $n = d \cdot 0 + n$, so $R \neq \emptyset$. Hence R has a minimum element $r \in R$ by the Well-Ordering Principle. In particular, we may write

* $[n = dq + r]$ for some $q \in \mathbb{N}_0$. (WTS: $0 \leq r < d$).

Assume, to the contrary, that $r \geq d$. Now

$r' = r - d \geq 0$ so $r' \in \mathbb{N}_0$ and $r' < r$ (because $d > 0$).

On the other hand $q' = q + 1 \in \mathbb{N}_0$. Now we compute

$$\begin{aligned} dq' + r' &= d(q+1) + (r-d) \\ &= dq + d + r - d \\ &= dq + r = n \end{aligned}$$

Thus $r' \in R$, but $r' < r = \min(R)$, which contradicts the fact r is minimum of R.

Hence $r \neq d$, i.e. $r < d$. Because $r \in \mathbb{N}_0$, we have $0 \leq r < d$ and $n = dq + r$, so we have proved the existence claim.

Uniqueness: Assume $n = dq + r$, $n = dq' + r'$, and $0 \leq r < d$ and $0 \leq r' < d$ for some $q, r, q', r' \in \mathbb{N}_0$.

(WTS: $q = q'$ and $r = r'$). Note that

$dq + r = n = dq' + r'$, so $d(q - q') + (r - r') = 0$ by subtracting RHS from LHS. On the other hand, $d(q - q') = r' - r$ and $q - q' \in \mathbb{Z}$, so $d \mid (r' - r)$ by definition of divisibility. In particular, $d \mid |r' - r|$. Now because $0 \leq r, r' < d$, we have $|r' - r| < d$

(because $r' < d$ and $-d < -r$, so $-d < r' - r < d$)

Hence, by a result from last lecture, $|r' - r| = 0$.

(a|b and a, b ≥ 0 and b < a, then b = 0.)

Hence $r' - r = 0$, so $r = r'$. At this point,

$$0 = d(q' - q) + (r' - r) = d(q' - q) + 0 = d(q' - q).$$

By the zero-product property, either $d = 0$ or $q' - q = 0$.

But $d > 0$, so $q' - q = 0$ and thus $q = q'$.

Hence we have both $q = q'$ and $r = r'$ as desired.

Hence the result follows. ∎